



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,089	01/11/2001	Thomas P. Donahue	4420-1	1077
25235	7590	11/29/2006		
HOGAN & HARTSON LLP ONE TABOR CENTER, SUITE 1500 1200 SEVENTEENTH ST DENVER, CO 80202			EXAMINER LAZARO, DAVID R	
			ART UNIT 2155	PAPER NUMBER

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/759,089

Applicant(s)

DONAHUE, THOMAS P.

Examiner

David Lazaro

Art Unit

2155

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 October 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6-10, 12-15, 17-36, 42, 44-59 and 61-68 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6-10, 12-15, 17-36, 42, 44-59, and 61-68 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in response to the amendment filed 10/04/2006.
2. Claims 1, 4, 19, 31, 33, 34, 42, 52, 54, 55, 64 and 68 were amended.
3. Claims 5, 11, 16, 37-41, 43 and 60 are canceled.
4. Claims 1-4, 6-10, 12-15, 17-36, 42, 44-59, and 61-68 are pending in this office action.

Response to Amendment

5. Applicant's arguments with respect to claims 1-4, 6-10, 12-15, 17-36, 42, 44-59, and 61-68 have been considered but are moot in view of the new ground(s) of rejection. The examiner address arguments that are still pertinent in the Response to Arguments section.
6. The rejections of Claims 1, 2, 6, 14, 27, 28, 29, 30 and 32 under 35 U.S.C. §112, second paragraph, are withdrawn.
7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 34 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claim 34 recites the limitation "the negative valued regular expressions" (emphasis added) in line 15. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 55-59 and 61 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,832,212 by Cragun et al. (Cragun).

13. With respect to Claim 55, Cragun teaches a method for monitoring and maintaining an acceptable use policy for computer network usage comprising:

capturing TCP/IP data on a network (Col.4 lines 36-50);

removing data content that does not contain language elements and storing a remaining content comprising a string of language elements separated by spaces

without regard to original formatting of the captured TCP/IP data (Col. 5 line 35 - Col. 6 line 30);

defining categories with weighted predetermined expressions, wherein the predetermined expressions are defined by a user (Col. 4 lines 9-16);

testing the remaining content for the presence of predetermined expressions (Col. 3 lines 54-65 and Col. 4 lines 30-50);

maintaining a sum of values associated with said predetermined expressions found within each category (Col. 4 lines 36-55);

storing the remaining data if the sum of values associated with said predetermined expressions present within a category exceeds a threshold value (Col. 4 lines 36-55).

14. With respect to Claim 56, Cragun further teaches said remaining data is stored only if the sum of predetermined expressions exceeds the threshold value in a plurality of categories (In Cragun: Col. 8 lines 15-39 - Super category).

15. With respect to Claim 57, Cragun further teaches wherein the threshold value for a category is defined as the presence of no predetermined expressions (In Cragun: Col. 4 lines 9-16 - user defined threshold).

16. With respect to Claim 58, Cragun further teaches wherein said computer network is a wide area network (In Cragun: Col. 3 lines 30-53).

17. With respect to Claim 59, Cragun further teaches wherein said computer network is a local area network (In Cragun: Col. 3 lines 30-53).

18. With respect to Claim 61, Cragun further teaches outputting a report relating to the presence of predetermined expressions whose sum meets or exceeds the threshold value of a category (In Cragun: Col. 5 lines 3-10).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. Claims 1-4, 6-8, 12-15, 17-33 and 65-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,453,345 by Trcka et al. (Trcka) in view of U.S. Patent 5,832,212 by Cragun et al. (Cragun) and U.S. Patent 6,266,664 by Russell-Falla et al. (Russell-Falla).

21. With respect to Claim 1, Trcka teaches in a computer network, a method for maintaining an acceptable use policy comprising:

receiving input from a user selecting criteria for use in monitoring network communications (Col. 13 lines 38-49 and Co. 17 line 56 - Col. 18 line 14);

monitoring TCP/IP network communications (Col. 2 lines 11-34, Col. 6 lines 1-12, Col. 7 lines 28-37);

storing raw TCP/IP session data of said TCP/IP network communications on disk (Col. 7 lines 14-27), even when the communication does not conform to a known protocol (Col. 2 lines 11-34, Col. 6 lines 1-25, Col. 7 lines 28-37)

testing the stored communications for the presence of at least one preselected criterion, wherein the preselected criterion is defined by a user, is associated with the user selected criteria (Col. 17 line 56 - Col. 18 line 14), and wherein the raw TCP/IP session data including all TCP control and payload data is tested for the presence of the at least one preselected criterion (Col. 6 lines 13-25 and Col. 7 lines 28-42 and Col. 18 lines 15-29 - the raw data includes all bit-level data which can be reconstructed and analyzed at any protocol level);

deleting the communications if the presence of the at least one preselected criterion is not determined (Col. 17 line 56 - Col. 18 line 14: tested data not matching the user defined preselected criterion is not stored in the database and is therefore deleted);

storing the communications if the presence of said at least one preselected criterion is predetermined (Col. 17 line 56 - Col. 18 line 14).

Trcka further teaches that the stored communications can be tested for the presence of a particular pattern or keyword (Col. 18 lines 43-46).

Trcka does not explicitly disclose that the input from a user is selecting a subject matter category such that the preselected criterion is associated with the user selected subject matter category, and comprises one or more regular expressions. Cragun teaches monitoring of TCP/IP network communications for particular categories of

content (Col. 2 lines 15-26; Col. 3 lines 30-53; and Col. 4 lines 36-50). In Cragun, a user selects a subject matter category for use in the monitoring (Col. 4 lines 9-18). The subject matter category is further associated with one or more word or word fragments (Col. 4 lines 9-18 and Col. 3 lines 54-65). While Trcka and Cragun do not disclose the use of regular expressions, Russell-Falla teaches that one or more words or regular expressions can be used to identify content as relating to a particular subject matter category (Col. 3 lines 1-9 and Col. 5 lines 7-12).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Trcka and modify it as indicated by Cragun and Russell-Falla such that it further comprises receiving input from a user selecting a subject matter category for use in monitoring network communications and testing the stored communications for the presence of at least one preselected criteria, wherein the preselected criterion is defined by a user, is associated with a user selected subject matter category, and comprises one or more regular expressions. One would be motivated to have this, as it is desirable to determine the subject matter category of network communications for protection and management purposes and to provide user control in relation to such purposes (In Russell-Falla: Col. 2 lines 24-35; In Cragun: Col. 2 lines 1-13).

22. With respect to Claim 2, Trcka further teaches wherein the preselected criterion comprises two or more subject matter categories (IN Cragun: Col. 2 lines 26-49).

23. With respect to Claim 3, Trcka further teaches wherein said subject matter categories comprise regular expressions (In Russell-Falla: Col. 3 lines 1-9 and Col. 5 lines 7-12).

24. With respect to Claim 4, Trcka further teaches wherein said regular expressions are assigned a weight by a user (In Cragun: Col. 4 lines 9-16).

25. With respect to Claim 6, Trcka further teaches wherein the preselected criterion is weighted (IN Cragun: Col. 4 lines 9-16 and lines 36-50).

26. With respect to Claim 7, Trcka further teaches wherein said regular expressions are weighted with either positive or negative values (IN Russell-Falla: Col. 3 line 59-Col. 4 line 3).

27. With respect to Claim 8, Trcka does not explicitly disclose wherein regular expressions within a subject matter category having a negative value are processed before regular expressions having a positive value.

Russell-Falla teaches the processing of regular expressions with both negative and positive values for a given subject matter category (Col. 5 lines 16-35). Based on the algorithm (Col. 5 line 25), it is mathematically arbitrary as to whether negative values are processed before positive values.

As such, It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Trcka and modify it as indicated by Russell-Falla such that the method further comprises wherein regular expressions within a subject matter category having a negative value are processed before regular expressions having a positive value. One would be motivated to have

Art Unit: 2155

this, as it is an arbitrary design choice since the overall sum determines the score (In Russell-Falla: Col. 5 lines 16-35).

28. With respect to Claim 12, Trcka further teaches wherein the computer network is a wide area network (IN Trcka: Col. 5 lines 50-67).

29. With respect to Claim 13, Trcka further teaches wherein the computer network is a local area network (IN Trcka: Col. 5 lines 50-67).

30. With respect to Claim 14, Trcka further teaches wherein the presence of the preselected criterion in at least one of said categories comprises a match in a plurality of categories (IN Cragun: Col. 8 lines 16-39 - category and super category).

31. With respect to Claim 15, Trcka further teaches wherein said subject matter categories comprise key words (Col. 4 lines 9-18 and Col. 3 lines 54-65).

32. With respect to Claim 17, Trcka further teaches assigning a threshold value to each subject matter category (In Cragun: Col. 4 lines 9-18; In Russell-Falla: Col. 5 lines 47-64).

33. With respect to Claim 18, Trcka further teaches wherein at least some of said subject matter categories comprises one or more predetermined expressions (In Cragun: Col. 3 lines 55-65 and Col. 4 lines 9-16; In Russell-Falla: Col. 3 lines 36-51).

34. With respect to Claim 19, Trcka further teaches receiving user input assigning a value to said predetermined expressions (In Cragun: Col. 4 lines 9-16).

35. With respect to Claim 20, Trcka further teaches summing the values of said predetermined expressions (In Cragun: Col. 4 lines 31-50; In Russell-Falla: Col. 3 line 60 - Col. 4 line 3).

36. With respect to Claim 21, Trcka further teaches said communication is further stored if the sum of values of said predetermined expressions comprising a subject matter category equal or exceed the threshold value assigned to said subject matter category (In Cragun: Col. 4 lines 51-55; In Trcka: Col. 17 line 56 - Col. 18 line 14).

37. With respect to Claim 22, Trcka further teaches wherein the threshold value of at least one subject matter category comprises equaling or exceeding the threshold value in a plurality of subject matter categories (In Cragun: Col. 8 lines 15-39 - Super category).

38. With respect to Claim 23, Trcka further teaches wherein said threshold values assigned to said subject matter categories are variable (In Cragun: Col. 4 lines 9-16).

39. With respect to Claim 24, Trcka further teaches wherein said subject matter categories have a hierarchical relationship (In Cragun: Col. 8 lines 15-39 - category and super category is hierarchical).

40. With respect to Claim 25, Trcka further teaches wherein said hierarchical relationship comprises defining the threshold value for at least one subject matter category as the presence of predetermined expressions in a plurality of other subject matter categories (In Cragun: Col. 8 lines 15-39 - category and super category is hierarchical).

41. With respect to Claim 26, Trcka further teaches wherein said hierarchical relationship comprises defining the threshold value for at least one subject matter category as matching or exceeding the threshold value assigned to a plurality of other

subject matter categories (In Cragun: Col. 8 lines 15-39 - category and super category is hierarchical).

42. With respect to Claim 27, Trcka further teaches outputting a report relating to the presence of said at least one preselected criterion (IN Trcka: Col. 18 lines 15-66).

43. With respect to Claim 28, Trcka further teaches wherein said report identifies individuals whose use of the computer network included communications which matched preselected criterion (In Trcka: Col. 23 lines 47-61 and Fig. 19 - user IDs related to the matched network event criterion are displayed).

44. With respect to Claim 29, Trcka further teaches wherein said report identifies network addresses where communications were received or originated that included matched preselected criterion (In Trcka: Col. 23 lines 47-61 and Fig. 19 - origin and destination address are reported)

45. With respect to Claim 30, Trcka further teaches outputting a report relating to the presence of preselected criterion, wherein said report identifies the number of matches in a category (In Cragun: Col. 10 lines 5-14)

46. With respect to Claim 31, Trcka further teaches wherein said report is in a graphical format and at least a portion of the stored communications is displayed in a user interface in a form matching that generated or viewed during the monitored TCP/IP network communication (In Trcka: Col. 18 lines 15-52 - the stored raw network data can be interpreted at a transaction level so as to display, example, an HTML page that appeared in transaction sequence).

47. With respect to Claim 32, Trcka further teaches wherein said report provides the text of all communications that match said preselected criterion (In Trcka: Col. 18 lines 15-52 - stored raw network data can be interpreted at a transaction level which allows for all textual content to be viewed as desired).

48. With respect to Claim 33, Trcka further teaches wherein said report is in a human readable format and at least a portion of the stored communications is provided in the report in a form matching that generated or viewed during the monitored TCP/IP network communications (In Trcka: Col. 18 lines 15-52 - the stored raw network data can be interpreted at a transaction level so as to display, example, an HTML page that appeared in transaction sequence).

49. With respect to Claim 65, Trcka further teaches wherein at least one stored half session comprises a plurality of independent parts, and the testing is performed individually on each independent part (In Trcka: Col. 18 lines 15-29 and Col. 7 lines 28-37 - any protocol level).

50. With respect to Claim 66, wherein the independent parts comprises individual emails (In Trcka: Col. 14 line 61 - Col. 15 line 9).

51. With respect to Claim 67, wherein the independent parts comprise message attachments (In Trcka: Col. 14 line 61 - Col. 15 line 9).

52. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka in view of Cragun and Russell-Falla as applied to claim 4 above, and further in view of U.S. Patent 5,878,423 by Anderson et al. (Anderson).

53. With respect to Claim 9, Ranum in view of Trcka and Russell-Falla does not explicitly disclose prioritizing the order which regular expressions within a subject matter category are tested.

Anderson teaches prioritization of the use of keywords with corresponding subject matter categories (Col. 11 lines 1-12 and lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Trcka in view of Cragun and Russell-Falla and modify it as indicated by Anderson such that the method further comprises prioritizing the order which regular expressions within a subject matter category are tested. One would be motivated to have this, as it improves searching by providing the more important and useful information first (In Anderson: Col. 11 lines 40-46).

54. With respect to Claim 10, Trcka in view of Cragun and Russell-Falla further teaches wherein said prioritizing reduces the likelihood of false hits (In Anderson: Col. 11 lines 40-46).

55. Claim 68 is rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka in view of Cragun and Russell-Falla and in further view of U.S. Patent 7,016,951 by Longworth et al. (Longworth).

56. With respect to Claim 68, Trcka in view of Cragun and Russell-Falla further teaches testing independent parts of stored TCP/IP network communications at any protocol level (In Trcka: Col. 18 lines 15-29 and Col. 7 lines 28-37 - any protocol level).

Trcka in view of Cragun and Russell-Falla does not explicitly disclose prior to the testing, attempting to identify a protocol by comparing the stored TCP/IP network communications with known protocol patterns, wherein when the attempting results in one of the known protocol patterns being identified, the testing of the stored communications involves testing each independent part of the stored TCP/IP network communications associated with the identified one of the known protocol patterns. Longworth teaches attempting to identify a protocol by comparing the stored TCP/IP network communications with known protocol patterns (Col. 6 lines 8-29). This includes a recursive process for protocols nested within other protocols (Col. 6 lines 30-44).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Trcka in view of Cragun and Russell-Falla and modify as indicated by Longworth such that it further comprises prior to the testing, attempting to identify a protocol by comparing the stored TCP/IP network communications with known protocol patterns, wherein when the attempting results in one of the known protocol patterns being identified, the testing of the stored communications involves testing each independent part of the stored TCP/IP network communications associated with the identified one of the known protocol patterns. One would be motivated to have this, as it provides for an enhanced analysis of network communications (In Longworth: Col. 2 lines 18-22).

57. Claims 34-36, 42, 44-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell-Falla in view of Trcka and Cragun.

With respect to Claim 34, Russell-Falla teaches capturing data on a network (Col. 4 line 61 – Col. 5 line 4) wherein the data comprises at least part of multiple half sessions of TCP/IP communications (HTML data would be part of multiple half sessions of TCP/IP communications -Col. 4 line 61 - Col. 5 line 21 and Col. 1 lines 37-45);

removing data content that does not contain language elements (Col. 5 lines 5-11 - the examiner considers the act of identifying and analyzing natural language elements to be within the scope of the limitation);

testing the remaining content for the presence of predetermined expressions (Col. 5 lines 5-11) wherein the predetermined expressions comprise two or more categories (Col. 4 lines 45-60 and Col. 9 lines 9-12) each containing predetermined expressions (Col. 5 lines 5-35);

maintaining a sum of values associated with said predetermined expressions found within at least one category (Col. 3 line 65 – Col. 4 line 3);

determining if the remaining data is within a category if the sum of values associated with said predetermined expressions within a category meets or exceeds a threshold value (Col. 5 lines 5-64);

wherein said expressions are weighted with either positive or negative values.

Russell-Falla does not explicitly state the negative valued expressions are tested first. However, based on the algorithm (Col. 5 line 25), it is mathematically arbitrary as to whether negative values are processed before positive values.

Russell-Falla does not explicitly disclose the captured data comprising complete multiple half sessions of TCP/IP network communications. Trcka teaches capturing

data on a network, wherein the data comprises multiple half sessions of TCP/IP network communications (Col. 2 lines 11-34, Col. 6 lines 1-12, Col. 7 lines 14-37). The multiple half sessions can be tested for user defined criterion (Col. 17 line 56 - Col. 18 line 14).

Russell-Falla does not explicitly disclose the predetermined expressions are defined by a user, that the data is stored when the data is determined to be within a category based on a sum of values, and that the testing and maintaining step are halted and the storing is performed when the sum of values within a category meets or exceeds the threshold value. Cragun teaches user defined expressions in a network monitoring system (Col. 3 lines 54-65 and Col. 4 lines 9-16). Cragun teaches the storing of data when the data is determined to be within a category based on a sum of values (Col. 4 lines 36-55). Cragun further teaches testing internet packets and maintaining of the sum of values is halted when the sum of values meets or exceeds a threshold value (Col.4 lines 58-63).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Russell-Falla and modify it as indicated by Trcka and Cragun such that it further comprises capturing data on a network, wherein the data comprises multiple half sessions of TCP/IP network communications; predetermined expressions that are defined by a user; and storing the remaining data if the sum of values associated with said predetermined expressions within a category meets or exceeds a threshold value selected based on user input; wherein negative valued regular expressions are tested first; and wherein the testing and the maintaining are halted and the storing is performed when the sum of values

within a category meets or exceeds the threshold value. One would be motivated to incorporate the teachings of Trcka and Cragun, as it is desirable to determine the subject matter category of network communications for protection and management purposes and to provide user control in relation to such purposes (In Russell-Falla: Col. 2 lines 24-35; In Cragun: Col. 2 lines 1-13). One would be motivated to test negative values first, as it is an arbitrary design choice since the overall sum determines the score (In Russell-Falla: Col. 5 lines 16-35).

58. With respect to Claim 35, Russell-Falla further teaches wherein the computer network is a wide area network (IN Trcka: Col. 5 lines 50-67).

59. With respect to Claim 36, Russell-Falla further teaches wherein the computer network is a local area network (IN Trcka: Col. 5 lines 50-67).

60. With respect to Claim 42, Russell-Falla does not explicitly state wherein said negative and positive valued regular expressions are separately tested in order of largest value to smallest value.

However, Russell-Falla teaches the processing of regular expressions with both negative and positive values for a given subject matter category (Col. 5 lines 16-35). Based on the algorithm (Col. 5 line 25), it is mathematically arbitrary as to whether the negative and positive valued regular expressions are separately tested in order of largest value to smallest value.

As such, It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Russell-Falla and modify it such that the method further comprises wherein said negative and positive valued

regular expressions are separately tested in order of largest value to smallest value.

One would be motivated to have this, as it is an arbitrary design choice since the overall sum determines the score (In Russell-Falla: Col. 5 lines 16-35).

61. With respect to Claim 44, Russell-Falla further teaches said expressions are regular expressions (Col. 3 lines 1-6 of Russell-Falla).

62. With respect to Claim 45, Russell-Falla further teaches wherein the threshold value of at least one category comprises meeting or exceeding the threshold value for a plurality of other categories (In Cragun: Col. 8 lines 15-39 - Super category).

63. With respect to Claim 46, Russell-Falla further teaches wherein the threshold value of at least one category comprises meeting or exceeding the threshold value for at least one other category and not meeting or exceeding the threshold value for at least another category (In Cragun: Col. 8 lines 15-39 - Super category).

64. With respect to Claim 47, Russell-Falla further teaches said threshold value for a category is variable (In Russell-Falla Col. 5 lines 47-63 of).

65. With respect to Claim 48, Russell-Falla further teaches outputting a report relating to the presence of predetermined expressions (In Russell-Falla Col. 6 lines 29-34 of).

66. With respect to Claim 49, Russell-Falla further teaches said report identifies individuals whose use of the computer network included communications which matched predetermined expressions (In Russell-Falla: Col. 6 line 29-34, note the functionality of the report in Russell-Falla is tied to a user; and In Trcka: Col. 23 lines

Art Unit: 2155

47-61 and Fig. 19 - user IDs related to the matched network event criterion are displayed).

67. With respect to Claim 50, Russell-Falla further teaches said report identifies network addresses where communications were received or originated that included matched predetermined expressions (In Trcka: Col. 23 lines 47-61 and Fig. 19 - origin and destination address are reported).

68. With respect to Claim 51, Russell-Falla further teaches outputting a report relating to the presence of predetermined expressions, wherein said report identifies the number of matches in a category (In Cragun: Col. 10 lines 5-14).

69. With respect to Claim 52, Russell-Falla further teaches wherein said report is in a graphical format and at least a portion of the stored communications is displayed in a user interface in a form matching that generated or viewed during the monitored TCP/IP network communication (In Trcka: Col. 18 lines 15-52 - the stored raw network data can be interpreted at a transaction level so as to display, example, an HTML page that appeared in transaction sequence).

70. With respect to Claim 53, Russell-Falla further teaches wherein said report provides the text of all communications that match said preselected criterion (In Trcka: Col. 18 lines 15-52 - stored raw network data can be interpreted at a transaction level which allows for all textual content to be viewed as desired).

71. With respect to Claim 54, Russell-Falla further teaches wherein said report is in a human readable format and at least a portion of the stored communications is provided in the report in a form matching that generated or viewed during the monitored TCP/IP

network communications (In Trcka: Col. 18 lines 15-52 - the stored raw network data can be interpreted at a transaction level so as to display, example, an HTML page that appeared in transaction sequence).

72. Claims 62 - 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cragun in view of Trcka.

73. With respect to Claim 62, Cragun does not explicitly disclose wherein said report identifies individuals whose use of the computer network included communications which contained predetermined expressions whose sum matched or exceeded the threshold value of at least one category.

Trcka teaches a report that identifies individuals whose use of the computer network included communications which contained predetermined criterion defined by a user (In Russell-Falla: Col. 6 line 29-34, note the functionality of the report in Russell-Falla is tied to a user; and In Trcka: Col. 23 lines 47-61 and Fig. 19 - user IDs related to the matched network event criterion are displayed).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Cragun and modify it as indicated by Trcka such that it further comprises wherein said report identifies individuals whose use of the computer network included communications which contained predetermined expressions whose sum matched or exceeded the threshold value of at least one category. One would be motivated to have this, as it is desirable to provide features

that allow the user to efficiently focus on network communications of interest (In Trcka: col. 18 lines 12-14 and lines 62-66; and Col. 20 lines 1-17).

74. With respect to Claim 63, Cragun does not explicitly disclose wherein said report identifies network addresses where communications were received or originated that included predetermined expressions whose sum matched or exceeded the threshold value of at least one category.

Trcka teaches a report that identifies network addresses where communications were received or originated that included predetermined criterion defined by a user (In Trcka: Col. 23 lines 47-61 and Fig. 19 - origin and destination address are reported).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Cragun and modify it as indicated by Trcka such that it further comprises wherein said report identifies network addresses where communications were received or originated that included predetermined expressions whose sum matched or exceeded the threshold value of at least one category. One would be motivated to have this, as it is desirable to provide features that allow the user to efficiently focus on network communications of interest (In Trcka: col. 18 lines 12-14 and lines 62-66; and Col. 20 lines 1-17).

75. With respect to Claim 64, Cragun does not explicitly disclose wherein said report is in a graphical format and at least a portion of the stored communications is displayed in a user interface in a form matching that generated or viewed during the monitored TCP/IP network communication.

Trcka teaches a report that is in a graphical format and at least a portion of the stored communications is displayed in a user interface in a form matching that generated or viewed during the monitored TCP/IP network communication (In Trcka: Col. 18 lines 15-52 - the stored raw network data can be interpreted at a transaction level so as to display, example, an HTML page that appeared in transaction sequence).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Cragun and modify it as indicated by Trcka such that it further comprises wherein said report is in a graphical format and at least a portion of the stored communications is displayed in a user interface in a form matching that generated or viewed during the monitored TCP/IP network communication. One would be motivated to have this, as it is desirable to provide features that allow the user to efficiently focus on network communications of interest (In Trcka: col. 18 lines 12-14 and lines 62-66; and Col. 20 lines 1-17).

Response to Arguments

76. On page 13 of the remarks, Applicant argues - *"In contrast, Trcka describes a simple filter mechanism... This filtering mechanism is applied to each data packet on an individual bases, and, as a result, ignores control data and would produce a very different result than a testing process that looks at multiple packets or data payload of a complete communication or session along with control data"*

- a. Examiner's response - Trcka captures data from the data link layer up which allows for an analysis of "all bit level data and headers of all packets transferred over the network, and thus includes all the information needed to fully reconstruct all network transactions" (emphasis added, Col.6 lines 13-15 of

Trcka). It is clear from this passage that applicants interpretation of Trcka is in error. Furthermore, Trcka describes the network data analysis as capable of extracting specific details from any particular layer or application level, which allows a user to examine the contents as originally generated or viewed during the session (Col. 18 lines 22-45). Applicant's arguments are not persuasive.

77. On page 17 of the remarks, Applicant argues - *"Trcka does not teach any specific type of analysis that would be performed on the raw data packets. Hence, Trcka does not teach the step of testing the stored communication for the presence of at least one user-defined criterion. Further, Trcka does not show monitoring TCP/IP network communications. Trcka stores raw data packets at a network communication at a data link or lower level (e.g., Ethernet packets or lower). This is data below the transport level, and below the TCP/IP level called for in claim 1. Further, claim 1 calls for storing the communication in a conditional manner, "if the presence of at least one preselected criterion is determined." Trcka teaches that all raw data packets are stored, not a process of storing some and deleting some as called for in claim 1."*

b. Examiner's response: Col. 17, lines 65 - Col. 18 line 14 of Trcka specifically calls for analysis of stored raw data packets such that they are tested for user specified criterion. The purposes of this testing is so that the database only stores "the traffic events of interest" to the user. No where does it mention the raw data packets are also stored database, therefore they must be deleted and the conditional manner of storing is present in Trcka.

c. The examiner agrees that the data link level is below the transport level. As such, any raw data packets captured at the data link level will have transport

level information encapsulated within each packet. This is the standard functionality of a protocol stack. Trcka captures raw network data at the data link level so that analysis can be performed to any particular protocol layer or application. Applicant's arguments are not persuasive.

78. On page 23 of the remarks, applicant argues - *"At col. 5, lines 5-11, Russel-Falla is said to teach 'the act of identifying and analyzing natural language elements', and the Examiner argues that this is within the scope of the removing data step of claim 34. However, such identifying does not indicate or teach that the other content was removed or that later the 'remaining data' is to be stored (i.e., not the removed content). Hence, the removing data content step is not shown by Russell-Falla."*

d. Examiner's response: It is clear that Russell-Falla only tests the language elements of the data being tested. Russell-Falla does not state testing of non-language elements. As a method step, it is clear that Russell-Falla identifies and only uses the language elements of the data and therefore removes data content that does not contain language elements from the testing procedure. Applicant's arguments are not persuasive.

Conclusion

79. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 571-272-3986. The examiner can normally be reached on 8:30-5:00 M-F.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Art Unit: 2155

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


David Lazaro
November 20, 2006


SALEH NAJJAR
SUPERVISORY PATENT EXAMINER